Medicare Learning Network
MLN Matters
CMS
Information for Medicare Fee-for-Service Health Care Professionals

Flu Shot Reminder

It's Not Too Late to Get the Flu Shot. We are in the midst of flu season and a flu vaccine is still the best way to prevent infection and the complications associated with the flu. But re-vaccination is necessary each year because the flu viruses change each year. Encourage your Medicare patients who haven't already done so to get their annual flu shot and don't forget to immunize yourself and your staff. Protect yourself, your patients, and your family and friends. Get Your Flu Shot. It's Not Too Late! Remember - Influenza vaccination is a covered Part B benefit. Note that influenza vaccine is NOT a Part D covered drug. For more information about Medicare's coverage of adult immunizations and educational resources, go to CMS's website: http://www.cms.hhs.gov/MLNMattersArticles/downloads/SE0667.pdf .

MLN Matters Number: MM5431 | Related Change Request (CR) #: 5431

Related CR Release Date: January 5, 2007 | Effective Date: January 1, 2007

Related CR Transmittal #: R1149CP | Implementation Date: April 2, 2007

Rules of Behavior Governing Medicare Eligibility Inquiries

Provider Types Affected

All providers and suppliers, including their third party billing agents or clearinghouses, who submit eligibility inquiries to Medicare

Provider Action Needed

STOP – Impact to You

The Centers for Medicare & Medicaid Services (CMS) is committed to maintaining the integrity and security of health care data in accordance with applicable laws and regulations. If you, or your biller, do not adhere to these rules of behavior and/or other CMS data privacy and security rules, you could incur revocation of access to the data as well as other penalties.

CAUTION – What You Need to Know

CR 5431, from which this article is taken, restates your responsibilities in obtaining, disseminating, and using beneficiary's Medicare eligibility data; and also delineates CMS' expectations for provider and clearinghouse use of the HIPAA 270/271 Extranet application.

GO – What You Need to Do

Read the key points from CR 5431 in the Background section, below, and make sure that your staffs read the manual section (*Medicare Claims Processing Manual* (100-04), Chapter 31 (ANSI X12N Formats Other than Claims or Remittance), Section 10.3 (Eligibility Rules of Behavior), attached to CR5431. (See Additional Information, below, for instructions in locating CR5431.)

Background

Disclosure of Medicare beneficiary eligibility data is restricted under the provisions of the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA.)

CR 5431, upon which this article is based, restates your responsibilities in obtaining, disseminating, and using beneficiary's Medicare eligibility data; and outlines CMS' expectations for providers and clearinghouses who use the HIPAA 270/271 Extranet application.

In October 2005, CMS began offering to Medicare providers and clearinghouses, the HIPAA 270/271 beneficiary eligibility transaction, real-time, via the CMS AT&T communication Extranet; and in June 2006, began to pilot an internet application for eligibility information. Over time, this application will be available to an increasing number of Medicare providers.

Please keep in mind that the Medicare Electronic Data Interchange (EDI) Enrollment process (which collects the information needed to successfully exchange EDI transactions between Medicare and EDI trading partners, and establishes the data exchange expectations for both), must be executed by each provider that submits/receives EDI either directly to or from Medicare or through a third party (a billing agent or clearinghouse).

First, here are the key points, from the CR, that address your responsibilities in dealing with beneficiary eligibility data.

- The HIPAA Privacy Rule mandates the protection and privacy of all health information, and specifically defines the authorized uses and disclosures of "individually-identifiable" health information. CMS is committed to maintaining the integrity and security of health care data in accordance with the applicable laws and regulations.
- You should always remember that Medicare eligibility data is to be used for Medicare business only, and that providers and their staffs are expected to use, and disclose, this protected health information according to the CMS regulations.

- Authorized purposes for requesting beneficiary Medicare eligibility information include:
  - To verify eligibility, after screening the patient to determine Medicare Part A or Part B eligibility;
  - To determine beneficiary payment responsibility with regard to deductible/co-insurance;
  - To determine eligibility for services such as preventive services;
  - To determine if Medicare is the primary or secondary payer;
  - To determine if the beneficiary is in the original Medicare plan, Part C plan (Medicare Advantage) or Part D plan; and
  - To determine proper billing.

Conversely, examples of unauthorized purposes for requesting beneficiary Medicare eligibility information include:

- To determine eligibility for Medicare without screening the patient to determine if they are Medicare eligible; or
- To acquire the beneficiary's health insurance claim number.

In dealing with Medicare beneficiary eligibility information, you and your employees/staff must:

- Ensure sufficient security measures exist to associate a particular transaction with a particular staff member or employee before requesting the information;
- Cooperate with CMS or its agents in the event that CMS has a security concern with respect to any eligibility inquiry;
- Promptly inform CMS or one of CMS's contractors (e.g., your carrier, fiscal intermediary (FI), or Part A/B Medicare Administrative Contractor (A/B MAC)) if you identify misuse of "individually-identifiable" health information accessed from the CMS database; and
- Limit each inquiry for Medicare beneficiary eligibility data to that for a patient that you are currently treating/serving, or who has contacted you about treatment or service, or for whom you have received a referral from a health care provider that has treated or served that patient.

Penalties

- HHS may impose civil money penalties on a HIPAA-covered entity of $100 per failure to comply with a Privacy Rule requirement (not to exceed $25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year).

- Further, a person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA or a trading partner agreement under 42 U.S.C 1320d-6 faces a fine of $50,000 and up to one-year imprisonment (increasing to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm).
- Under the False Claims Act, anyone who knowingly submits, or causes another person or entity to submit, false claims for payment of government funds is liable for three times the government's damages plus civil penalties of $5,500 to $11,000 per false claim.

CR5431 also discusses CMS' expectations for providers and Clearinghouses who use the HIPAA 270/271 Extranet application. A synopsis of this discussion follows.

For Providers

In order to access and use this system, you will need to 1) Register, on line, in IACS (Individual Authorized Access to CMS Computer Services) and provide your social security number and e-mail address so that the system can identify you and communicate with you through email, if necessary; and 2) Adhere to basic desktop security measures and to the CMS computer systems security requirements in order to ensure the security of Medicare beneficiary personal health information.

You will also be required to adhere to the security requirements for users of CMS computer systems and to the basic desktop security measures to ensure the security of Medicare beneficiary personal health information. You must not:

- Disclose or lend your identification number and/or password to someone else. They are for your use only and serve as your electronic signature. This means that you may be held responsible for the consequences of unauthorized or illegal transactions.
- Browse or use CMS data files for unauthorized or illegal purposes.
- Use CMS data files for private gain or to misrepresent yourself or CMS.
- Make any disclosure of CMS data that is not specifically authorized.

As mentioned earlier, violation of these security requirements could result in termination of system access privileges and /or disciplinary/adverse action up to and including legal prosecution.

For Clearinghouses

CMS allows the release of eligibility data to third parties (providers' authorized billing agents or Clearinghouses) for the purpose of preparing an accurate Medicare claim or determining eligibility for specific services.

In order to receive such access on behalf of providers, billing agents/Clearinghouses must adhere to the following rules:

- Such entities may not submit an eligibility inquiry except as a health care provider's authorized, and through a business associate contract with the provider;
- Each provider that contracts with a billing agent/clearinghouse must sign a valid EDI Enrollment Form and be approved by a Medicare contractor before eligibility data can be sent to the third party;
- Each billing agent/clearinghouse must sign appropriate agreement(s) (i.e. Rules of Behavior, Trading Partner Agreement and Attestation Form) directly with CMS and/or one of CMS's contractors; and
- The billing agent/clearinghouse must be able to associate each inquiry with the provider or billing service making the inquiry.

Additional Information

You can find more information about the rules of behavior with respect to obtaining, disseminating, and using beneficiary's Medicare eligibility data by going to CR 5431, located at http://www.cms.hhs.gov/Transmittals/downloads/R1149CP.pdf on the CMS website; and reading the attached *Medicare Claims Processing Manual* (100-04), Chapter 31 (ANSI X12N Formats Other than Claims or Remittance), Section 10.3(Eligibility Rules of Behavior).

If you have any questions, please contact your carrier, fiscal intermediary (FI), regional home health intermediary (RHHI), A/B MAC, Durable Medical Equipment Regional Carrier (DMERC) or DME MAC at their toll-free number, which may be found at http://www.cms.hhs.gov/MLNProducts/downloads/CallCenterTollNumDirectory.zip.